Groupe de travail Réseau
Request for Comments : 4208
Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

G. Swallow, Cisco Systems, Inc
J. Drake, Boeing
H. Ishimatsu, G1M Co., Ltd.
Y. Rekhter, Juniper Networks, Inc
octobre 2005

Interface usager-réseau (UNI) de commutation généralisée d'étiquettes multi protocoles (GMPLS) : prise en charge du protocole de réservation de ressource - ingénierie du trafic (RSVP-TE) pour le modèle de recouvrement

Statut de ce mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

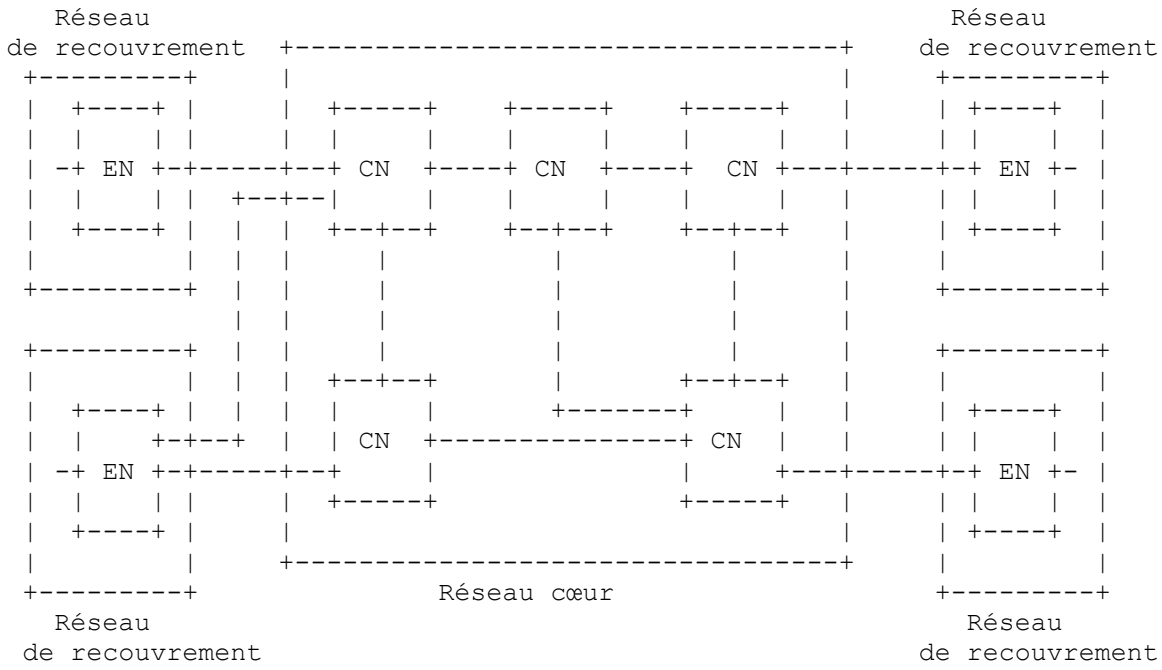
La commutation d'étiquettes multi protocoles généralisée (GMPLS, *Generalized Multiprotocol Label Switching*) définit des protocole d'acheminement et de signalisation pour la création de chemins de commutation d'étiquettes LSP, *Label Switched Path*) dans diverses technologies de commutation. Ces protocoles peuvent être utilisés pour prendre en charge un certain nombre de scénarios de déploiement. Le présent mémoire vise l'application de GMPLS au modèle de recouvrement.

Table des Matières

1. Introduction

La commutation d'étiquettes multi protocoles généralisée (GMPLS, *Generalized Multiprotocol Label Switching*) définit des protocoles d'acheminement et de signalisation pour la création de chemins de commutation d'étiquettes (LSP, *Label Switched Path*) dans diverses technologies de commutation. Ces protocoles peuvent être utilisés pour prendre en charge un certain nombre de scénarios de déploiement. Dans un modèle homologue, les nœuds de bordure prennent en charge aussi bien un protocole d'acheminement que un protocole de signalisation. Les interactions de protocole entre un nœud de bordure et un nœud cœur sont les mêmes que entre deux nœuds cœurs. Dans le modèle de recouvrement, les nœuds cœurs

agissent plus comme un système clos. Les nœuds de bordure ne participent pas à l'instance de protocole d'acheminement qui court entre les nœuds cœurs ; en particulier, les nœuds de bordure ne connaissent pas la topologie des nœuds cœurs. Il peut cependant y avoir une interaction de protocole d'acheminement entre un nœud cœur et un nœud de bordure pour l'échange d'informations d'accessibilité avec les autres nœuds de bordure.



Légende :
EN *(Edge Node)* nœud de bordure
CN *(Core Node)* nœud cœur

Figure 1: Modèle de référence de recouvrement

La Figure 1 montre un réseau de référence. Le réseau cœur est représenté par la grosse boîte au centre. Elle contient cinq nœuds cœurs marqués 'CN'. Les quatre boîtes autour du bord marquées "Réseau de recouvrement" représentent quatre îlots d'un seul réseau de recouvrement. Seuls les nœuds de ce réseau qui ont des liaisons TE dans le réseau cœur sont montrés. Ces nœuds sont appelés "nœuds de bordure" ; la terminologie est par rapport au réseau cœur, et non au réseau de recouvrement. Noter que chaque boîte marquée "Réseau de recouvrement" pourrait contenir beaucoup d'autres nœuds. Ces nœuds ne sont pas montrés, ils ne participent pas directement à la signalisation décrite dans le présent document. Seuls les nœuds de bordure peuvent signaler pour l'établissement de liaisons à travers le cœur aux autres nœuds de bordure.

Il sort du domaine d'application du présent document de décrire comme est demandée et déclenchée une liaison entre nœuds de bordure, ainsi que la façon précise dont cette liaison est utilisée par le réseau de recouvrement. Une possibilité est que les nœuds de bordure informent les autres nœuds du réseau de recouvrement de l'existence de la liaison, éventuellement en utilisant une adjacence de transmission comme décrit dans la [RFC4206]. Noter que ceci diffère d'une adjacence de transmission qui est fournie par le réseau cœur comme une liaison entre nœuds cœurs.

Dans le modèle de recouvrement, il peut y avoir des restrictions sur ce qui peut être signalé entre un nœud de bordure et un nœud cœur. Le présent mémoire s'adresse à l'application de GMPLS au modèle de recouvrement. Précisément, il traite des procédures RSVP-TE entre un nœud de bordure et un nœud cœur dans le modèle de recouvrement. Toutes les procédures de signalisation sont identiques aux extensions à GMPLS spécifiées dans la [RFC3473], sauf comme noté dans le présent document.

Le présent document s'occupe principalement des interactions entre un nœud de bordure et son nœud cœur adjacent (au plan des données) ; des capacités de signalisation hors bande et non adjacente peuvent signifier que les messages de signalisation sont livrés sur un chemin plus long. Sauf quand c'est noté autrement, le terme nœud cœur se réfère au nœud immédiatement adjacent à un nœud de bordure à travers une interface de plan de données particulière. Le terme de nœud cœur, se réfère cependant à tous les nœuds dans le cœur.

La réalisation d'une seule ou de plusieurs instance de l'UNI dépend de la mise en œuvre aussi bien au CN qu'à l'EN pour autant qu'elle satisfasse aux exigences fonctionnelles de robustesse, sécurité, et confidentialité décrites à la Section 7.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Le lecteur est supposé familiarisé avec la terminologie introduite dans les [RFC3031], [RFC3945], et [RFC3471].

1.1 Interface usager-réseau GMPLS (GMPLS UNI)

On peut appliquer le modèle de recouvrement GMPLS au point de référence d'interface usager réseau (UNI, *User-Network Interface*) défini dans le réseau optique à commutation automatique (ASON, *Automatically Switched Optical Network*) [G.8080]. Considérons le cas où le "Réseau cœur" de la Figure 1 est un réseau de fournisseur d'accès, et les nœuds de bordure sont des appareils "d'utilisateur". L'interface entre un EN et un CN est le point de référence UNI, et pour prendre en charge le modèle ASON, on doit définir la signalisation à travers l'UNI.

Les extensions décrites dans ce mémoire fournissent des mécanismes pour la signalisation d'UNI qui sont compatibles avec la signalisation GMPLS [RFC3471], [RFC3473]. De plus, ces mécanismes pour la signalisation d'UNI sont en ligne avec le modèle RSVP ; à savoir qu'il y a une seule session RSVP de bout en bout pour la connexion d'utilisateur. Le premier et le dernier bond constituent l'UNI, et la session RSVP porte les paramètres d'utilisateur de bout en bout. Cela évite d'avoir à transposer (ou porter) les paramètres d'utilisateur dans le format attendu par l'interface de réseau à réseau (NNI, *network-to-network interface*) utilisée au sein du réseau du fournisseur d'accès. Cela à son tour signifie que l'UNI et la NNI peuvent être indépendantes l'une de l'autre, ce qui est une exigence de l'architecture ASON. Cependant, dans le cas où l'UNI et la NNI sont toutes deux du GMPLS fondé sur RSVP, la méthodologie spécifiée dans le présent mémoire permet qu'une seule session RSVP instancie les deux signalisations d'UNI et de NNI, si on le désire, et si c'est permis par la politique du fournisseur de service.

2. Adressage

Les adresses pour les nœuds de bordure dans le modèle de recouvrement sont tirées du même espace d'adresses que celui que les nœuds de bordure utilisent pour s'adresser à leurs nœuds cœurs adjacents. Ce peut être le même espace d'adresses que celui utilisé par les nœuds cœurs pour communiquer entre eux, ou ce peut être un espace de VPN pris en charge par les nœuds cœurs comme un recouvrement.

Pour être plus précis, un nœud de bordure et son nœud cœur de rattachement doivent partager le même espace d'adresses qui est utilisé par GMPLS pour la signalisation entre les nœuds de bordure à travers le réseau cœur. Un ensemble de tuples <nœud de bordure, nœud cœur> partage le même espace d'adresses si les nœuds de bordure dans l'ensemble pourraient établir entre eux des LSP (à travers les nœuds cœurs) sans transposition ni traduction d'adresse (noter que les nœuds de bordure dans l'ensemble peuvent être un sous ensemble de tous les nœuds de bordure). L'espace d'adresses utilisé par les nœuds cœurs pour communiquer entre eux peut, mais sans obligation, être partagé avec l'espace d'adresses utilisé par tout tuple <nœud de bordure, nœud cœur>. Cela n'implique pas une transposition biunivoque obligatoire entre un ensemble de LSP et un certain espace d'adressage.

Lorsque plusieurs réseaux de recouvrement sont pris en charge par un seul réseau cœur, un ou plusieurs espaces d'adresses peuvent être utilisés en fonction des exigences de confidentialité. Cela peut être réalisé sans faire varier les adresses du nœud cœur car c'est le tuple <nœud de bordure, nœud cœur> qui constitue l'adhésion d'espace d'adresses.

Un nœud de bordure est identifié soit par une seule adresse IP représentant son identifiant de nœud, soit par une ou plusieurs liaisons TE numérotées qui connectent le nœud de bordure aux nœuds cœurs. Les nœuds cœurs sont supposés ignorer les autres adresses associées à un nœud de bordure (c'est-à-dire, les adresses qui ne sont pas utilisées dans les connexions de signalisation à travers le cœur GMPLS).

Un nœud de bordure a seulement besoin de connaître sa propre adresse, une adresse du nœud cœur adjacent, et de connaître (ou être capable de résoudre) l'adresse de tout autre nœud de bordure auquel il souhaite se connecter, ainsi (bien sûr) que les adresses utilisées dans l'îlot de réseau de recouvrement dont il fait partie.

Un nœud cœur a seulement besoin de connaître (et tracer) les adresses sur les interfaces entre ce nœud cœur et ses nœuds de bordure rattachés, ainsi que les identifiants de nœud de ces nœuds de bordure. En plus, un nœud cœur a besoin de connaître les adresses d'interface et les identifiants de nœud des autres nœuds de bordure auxquels il est permis à un nœud de bordure rattaché de se connecter.

Lorsque il forme un SENDER_TEMPLATE, le nœud de bordure d'entrée inclut soit un identifiant de nœud, soit l'adresse d'une de ses liaisons TE numérotées. Dans le premier cas, la connexion ne sera faite que sur cette interface.

Lorsque il forme un SESSION_OBJECT, le nœud de bordure d'entrée inclut soit l'identifiant de nœud de l'appareil bordure de sortie, soit l'adresse d'une des liaisons TE numérotées de la sortie. Dans le premier cas, la connexion ne sera faite que sur cette interface. L'identifiant de tunnel étendu de l'objet SESSION est réglé soit à zéro, soit à une adresse de l'appareil bordure d'entrée.

Les liaisons peuvent être numérotées ou non numérotées. De plus, les liaisons peuvent être en faisceau *(bundled)* ou non. Voir les [RFC3945], [RFC3471], [RFC4201], et [RFC3477].

3. Traitement d'ERO

Un nœud de bordure PEUT inclure un objet Chemin explicite (ERO, *Explicit Route Object*). Un nœud cœur PEUT rejeter un message Path qui contient un ERO. Ce comportement est contrôlé par la configuration (et est heureusement cohérent avec elle). Si un nœud cœur rejette un message Path à cause de la présence d'un ERO, il DEVRAIT retourner un message PathErr avec un code d'erreur de "Classe d'objet inconnue" à l'envoyeur comme décrit dans la [RFC3209]. Cela cause l'échec de l'établissement de chemin.

De plus, un nœud cœur PEUT accepter les ERO qui incluent seulement le nœud de bordure d'entrée, le nœud cœur d'entrée, le nœud cœur de sortie, et le nœud de bordure de sortie. C'est pour la prise en charge du contrôle explicite d'étiquette sur l'interface de nœud de bordure ; voir ci-dessous. Si un nœud cœur rejette un message Path à cause de la présence d'un ERO qui n'a pas le format permis, il DEVRAIT retourner un message PathErr avec un code d'erreur de "Mauvais objet Chemin explicite" comme défini dans la [RFC3209].

3.1 Message Path sans ERO

Quand un nœud cœur reçoit un message Path d'un nœud de bordure qui ne contient pas d'ERO, il DOIT calculer un chemin pour la destination et inclure ce chemin dans un ERO, avant de transmettre le message Path. Une exception serait si le nœud de bordure de sortie était aussi adjacent à ce nœud cœur. Si aucun chemin n'est trouvé, le nœud cœur DEVRAIT retourner un message PathErr avec un code d'erreur et une valeur de 24,5 - "Aucun chemin disponible pour la destination".

3.2 Message Path avec ERO

Quand un nœud cœur reçoit un message Path d'un nœud de bordure qui contient un ERO, il DEVRAIT vérifier le chemin dans sa base de données topologiques avant de transmettre le message Path. Si le chemin n'est pas viable (conformément à la topologie, les ressources actuellement disponibles, ou la politique locale) un message PathErr avec un code d'erreur et une valeur de 24,5 - "Aucun chemin disponible pour la destination" devrait être retourné.

3.3 Contrôle explicite d'étiquette

Afin de prendre en charge le contrôle d'étiquette explicite et la pleine identification de la liaison de sortie, un nœud de bordure d'entrée peut inclure ces informations dans le ERO qu'il passe à son nœud cœur du voisinage. Dans le cas où aucun autre ERO n'est fourni, ces informations de contrôle explicites sont fournies comme le seul bond de l'ERO et son codées en réglant le premier sous objet de l'ERO à l'identifiant de nœud du nœud cœur de sortie avec le bit L établi ; suivant ce sous objet sont tous les autres sous objets nécessaires pour identifier la liaison et étiquettes comme ils apparaîtraient normalement.

Les mêmes règles s'appliquent à la présence des sous objets de contrôle explicite comme dernier bond dans l'ERO, si un ERO plus complet est fourni par le nœud de bordure d'entrée à son nœud cœur voisin ; mais dans ce cas, le bit L PEUT être à zéro.

Ce traitement est décrit dans les [RFC3473] et[RFC4003].

4. Traitement de RRO

Un nœud de bordure PEUT inclure un objet Enregistrement de chemin (RRO). Un nœud cœur PEUT supprimer le RRO d'un message Path avant de le transmettre. De plus, le nœud cœur peut supprimer le RRO d'un message Resv avant de le transmettre au nœud de bordure. Ce comportement est contrôlé par (et est cohérent avec) la configuration.

De plus, un nœud cœur PEUT éditer le RRO dans un message Resv de façon à n'y inclure que les sous objets provenant du nœud cœur de sortie jusqu'au nœud de bordure de sortie. C'est pour permettre au nœud d'entrée de savoir quelles sont la liaison et les étiquettes choisies à l'extrémité distante de la connexion.

5. Notification

Un nœud de bordure PEUT inclure un objet NOTIFY_REQUEST dans les messages Path et Resv qu'il génère. Les nœuds cœurs peuvent envoyer des messages Notify aux nœuds de bordure qui ont inclus l'objet NOTIFY_REQUEST.

Un nœud cœur PEUT supprimer un objet NOTIFY_REQUEST d'un message Path ou Resv reçu d'un nœud de bordure avant de le transmettre.

Si aucun objet NOTIFY_REQUEST n'est présent dans le message Path ou Resv reçu d'un nœud de bordure, le nœud cœur adjacent au nœud de bordure peut inclure un objet NOTIFY_REQUEST et régler sa valeur à sa propre adresse.

Dans l'un et l'autre des cas ci-dessus, le nœud cœur NE DEVRAIT PAS envoyer de messages Notify au nœud de bordure.

Quand un nœud cœur reçoit un objet NOTIFY_REQUEST d'un nœud de bordure, il PEUT mettre à jour l'adresse de nœud Notify avec sa propre adresse avant de le transmettre. Dans ce cas, quand les messages Notify sont reçus, ils PEUVENT être transmis de façon sélective (sur la base de la politique locale) au nœud de bordure.

6. Suppression de connexion

6.1 Suppression de connexion sans alarme

RSVP-TE supprime actuellement les connexions en utilisant soit un seul message PathTear, soit une combinaison des messages ResvTear et PathTear. À réception du message PathTear, un nœud supprime l'état de connexion et transmet le message. Dans les réseaux optiques, il est cependant possible que la suppression d'une connexion (par exemple, suppression du brasseur) dans un nœud peut être cause que la connexion soit perçue comme défaillante dans les nœuds vers l'aval (par exemple, perte de trame, perte de lumière, etc.). Cela peut à son tour conduire à des alarmes de gestion et peut-être au déclenchement de la restauration/protection pour la connexion.

Pour régler de problème, la procédure de suppression en douceur de connexion DEVRAIT être suivie. Dans cette procédure, un objet ADMIN_STATUS DOIT être envoyé dans un message Path ou Resv le long du chemin de la connexion pour informer tous les nœuds sur le chemin de la suppression prévue, avant la suppression réelle de la connexion. La procédure est décrite dans la [RFC3473].

Si un nœud cœur d'entrée reçoit un PathTear sans avoir vu auparavant un objet ADMIN_STATUS l'informant que la connexion va être supprimée, il PEUT mettre en pause le PathTear et envoyer d'abord un message Path avec un objet ADMIN_STATUS pour informer tous les LSR en aval que la connexion va être supprimée. Quand le Resv est reçu en écho au ADMIN_STATUS, ou en utilisant un temporisateur comme décrit dans la [RFC3473], le nœud cœur d'entrée DOIT transmettre le PathTear.

6.2 Suppression de connexion avec PathErr

La [RFC3473] introduit le fanion Path_State_Removed dans un message PathErr pour indiquer que l'envoyeur a supprimé tout l'état associé au LSP et n'a pas besoin de voir un PathTear. Un nœud cœur voisin d'un nœud de bordure PEUT transposer entre suppressions en utilisant ResvTear/PathTear et PathErr avec Path_state_Removed.

Un nœud cœur voisin d'un nœud de bordure qui reçoit un ResvTear de son voisin aval PEUT répondre par un PathTear et envoyer un PathErr avec Path_State_Removed plus loin en amont.

Noter, cependant, qu'un nœud cœur à côté d'un nœud de bordure qui reçoit un PathErr avec Path_State_Removed de son voisin aval NE DOIT PAS conserver l'état Path et envoyer un ResvTear plus loin en amont parce que cela impliquerait que l'état Path plus loin en aval a aussi été conservé.

7. Connexions de VPN

Comme indiqué dans la section Adressage, les extensions dans le présent document sont conçues comme compatibles avec le support des VPN. Comme le réseau cœur peut être d'une technologie autre que GMPLS, aucun moyen obligatoire de transposition des connexions du cœur pour accéder aux connexions n'est spécifié. Cependant, quand GMPLS est utilisé pour le réseau cœur, il est RECOMMANDÉ que la procédure suivante fondée sur la [RFC4206] soit suivie.

La connexion VPN est modélisée comme ayant trois bonds. Un pour chaque liaison d'accès et un bond à travers le réseau cœur.

La connexion VPN est établie en utilisant une procédure en deux étapes. Quand un message Path est reçu à un nœud cœur sur une interface qui fait partie d'un VPN, le message Path est conservé jusqu'à ce qu'une connexion de cœur soit établie.

La connexion à travers le cœur est établie comme un échange de signalisation séparé entre les nœuds cœurs, en utilisant l'espace d'adresses des nœuds cœurs. Pendant que cet échange est en cours, le message Path d'origine est conservé au nœud cœur d'entrée. Une fois l'échange achevé pour la connexion de cœur, cette connexion est utilisée dans la connexion VPN comme si c'était une seule liaison. Ceci est signalé en incluant un objet IF_ID RSVP_HOP (défini dans la [RFC3473]) en utilisant les procédures définies dans la [RFC4206].

Le message Path d'origine est alors transmis au sein du domaine d'adressage du VPN au nœud cœur rattaché au nœud de bordure de destination. De nombreuses façon de réaliser cela sont disponibles, incluant des tunnels IP et GRE et des VPN BGP/MPLS. Il sort du domaine d'application du présent document de spécifier un moyen particulier.

8. Considérations sur la sécurité

Le modèle de confiance entre les nœuds cœur et de bordure est différent de celui décrit dans la [RFC3473] car il est permis au cœur de cacher sa topologie aux nœuds de bordures, et il est permis au cœur de restreindre les actions des nœuds de bordure en filtrant des objet RSVP spécifiques.

9. Remerciements

Les auteurs tiennent à remercier Kireeti Kompella, Jonathan Lang, Dimitri Papadimitriou, Dimitrios Pendarakis, Bala Rajagopalan, et Adrian Farrel de leurs commentaires et apports. Merci de leur relecture attentive à Loa Andersson et Dimitri Papadimitriou.

Adrian Farrel a édité les deux dernières révisions de ce document pour incorporer les commentaires du dernier appel et de la relecture du groupe de travail.

10. Références

10.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3209] D. Awduche, et autres, "RSVP-TE : Extensions à RSVP pour les tunnels LSP", décembre 2001. (*Mise à jour par* RFC3936, RFC4420, RFC4874, RFC5151, RFC5420, RFC6790)

[RFC3471] L. Berger, éd., "Commutation d'étiquettes multi-protocoles généralisée (GMPLS) : description fonctionnelle de la signalisation", janvier 2003. (*MàJ par* RFC4201, RFC4328, RFC4872, RFC8359) *(P.S.)*

[RFC3473] L. Berger, "Extensions d'ingénierie de protocole - trafic de signalisation de réservation de ressource (RSVP-

TE) de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", janvier 2003. *(P.S., MàJ par 4003, 4201, 4420, 4783, 4784, 4873, 4974, 5063, 5151,* 8359)

10.2 Références pour information

[G.8080] Recommandation UIT-T G.8080/Y.1304, "Architecture pour le réseau optique à commutation automatique (ASON)," novembre 2001 (et révision, janvier 2003). voir http://www.itu.int.

[RFC3031] E. Rosen, A. Viswanathan, R. Callon, "Architecture de commutation d'étiquettes multi protocoles", janvier 2001. *(P.S.)* (*MàJ par la* RFC6790)

[RFC3477] K. Kompella, Y. Rekhter, "Signalisation des liaisons non numérotées dans le protocole de réservation de ressource – ingénierie du trafic (RSVP-TE)", janvier 2003. *(P.S.)*

[RFC3945] E. Mannie, éd., "Architecture de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", octobre 2004. *(P.S.)*

[RFC4003] L. Berger, "Procédure de signalisation GMPLS pour contrôle de sortie", février 2005. *(P.S.)*

[RFC4201] K. Kompella et autres, "Faisceaux de liaisons dans l'ingénierie du trafic MPLS", octobre 2005. *(P.S.)*

[RFC4206] K. Kompella, Y. Rekhter, "Hiérarchie de chemins commutés par étiquettes (LSP) avec l'ingénierie de trafic (TE) de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. *(P.S.)*

Adresse des auteurs

George Swallow
Cisco Systems, Inc.
1414 Massachusetts Ave,
Boxborough, MA 01719
téléphone : +1 978 936 1398
mél : swallow@cisco.com

John Drake
Boeing Satellite Systems
2300 East Imperial Highway
El Segundo, CA 90245
téléphone : +1 412 370-3108
John.E.Drake2@boeing.com

Hirokazu Ishimatsu
G1M Co., Ltd.
Nishinippori Start up Office 214,
5-37-5 Nishinippori, Arakawaku,
Tokyo 116-0013, Japan
mél : hirokazu.ishimatsu@g1m.jp

Yakov Rekhter
Juniper Networks, Inc.
mél : yakov@juniper.net

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.